Presented at 8th Intl. Conf. on IT Security Incident Management and IT Forensics, May 12-14, 2014. Published in the proceedings, ISBN 978-1-4799-4330-2.

Information security incident management: Planning for failure

Maria B. Line*†, Inger Anne Tøndel† and Martin G. Jaatun†

*Department of Telematics
Norwegian University of Science and Technology (NTNU)
N-7491 Trondheim, Norway
maria.b.line@item.ntnu.no

†SINTEF ICT
N-7465 Trondheim, Norway
{inger.a.tondel, martin.g.jaatun}@sintef.no

Abstract

This paper reports on an interview study on information security incident management that has been conducted in organizations operating industrial control systems that are highly dependent on conventional IT systems. Six distribution service operators from the power industry have participated in the study. We have investigated current practice regarding planning and preparation activities for incident management, and identified similarities and differences between the two traditions of conventional IT systems and industrial control systems. The findings show that there are differences between the IT and ICS disciplines in how they perceive an information security incident and how they plan and prepare for responding to such. The completeness of documented plans and procedures for incident management varies. Where documentation exists, this is in general not well-established throughout the organization. Training exercises with specific focus on information security are rarely performed. There is a need to create a more unified approach to information security incident management in order for the power industry to be sufficiently prepared to meet the challenges posed by Smart Grids in the near future.

Index Terms

Industrial control systems, Information security, Information technology, Incident management, Power industry, Smart grids

I. Introduction

Information technology (IT)[1] is permeating all levels of industrial control systems (ICS)[2]. The two traditions of IT and ICS differ in several aspects, like terminology, security culture, security requirements, and technologies used [1]. As an example, if a computer is infected by malware, the most common response is to disconnect the computer from the network and reinstall it. The priority is on removing the malware, sacrificing the availability of the computer. In an ICS, availability is the top priority. Shutting down a component may have a significant economic cost.

Industrial control systems (ICS) are frequently used for controlling physical objects, such as oil installations, railway signalling systems, or power production systems. An ICS is often safety-critical, as a malfunctioning ICS may have severe consequences for the physical environment [2]. In the near future, if not already, ICS will consist mainly of ”regular” IT components. The two traditions of IT and ICS will then need to collaborate in order to ensure continuous operation of the systems and uninterrupted power supply. The information security incident management process should therefore be integrated with safety procedures and procedures for responding to industrial accidents at the installation.

An information security incident management process consists of different phases; preparations, responding to an incident, and post-incident evaluations and improvements [3]. Benefits of a structured approach to infomation security incident management include [3] an overall improvement of information security, reduced impact of incidents, improved focus and better prioritization of security acticities, and better and more updated information security risk assessment efforts.

We have performed a study to investigate how information security incident management is performed in organizations operating industrial control systems, more specifically in distribution system operators (DSOs) in the power industry[3]. DSOs own and manage the power distribution grid[4]. They are selected as the domain of study due to the advent of the Smart Grid, which causes the integration of IT and ICS to take several steps further [1]. For consumers, the most obvious aspect of the Smart

[1]in many contexts also referred to as Information and Communication Technology (ICT)

[2]Several terms are used interchangably to denote such systems: industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA), process control systems, automation systems. Throughout this paper the term *control systems* and/or *ICS* will be used.

[3]This work is funded partially by the Norwegian Research Council through the *DeVID* project, grant no 217528, and partially by the Norwegian University of Science and Technology through the project *Smart Grids as a Critical Infrastructure*

[4]The distribution grid is low voltage part of the power grid, the part that transports power into every single household and power consumer.

Grid is the introduction of smart meters, but the DSOs are faced with many other IT challenges that include and go beyond the Advanced Metering Infrastructure (AMI). The increased reliance on conventional IT systems in this sector represents a paradigm shift in that personnel who have traditionally focused on safety aspects of power electronics, and ensuring sufficient delivery of electricity to consumers, now also have to worry about information security of their newly internet-enabled control systems.

The following research questions were defined for this part of our study:

- How are planning and preparatory activities for information security incident management performed by organizations depending on successful cooperation between IT systems and ICS?
- What differences can be found in how the planning and preparatory activities are performed for IT systems compared to ICS?

Identifying the practices both for the IT systems and the control systems is valuable to see which practices should be strengthened and further developed in a collaboration. People working with these systems have different experiences and competence, and it would be reasonable to think that there should be synergy effects by achieving increased cooperation.

Preliminary results from this study were presented by Line [4]. This paper is more comprehensive in all sections compared to the previous conference paper; a larger number of empirical studies are referred to as background, and the method is described in more detail, especially the industrial case context. The preliminary results were written up before a thorough analysis was performed. This analysis now forms the basis for the Findings and Discussion sections in this paper. However, the findings presented are related to the planning and preparation activities only, as opposed to the preliminary results, which covered all phases as described in ISO 27035. In this paper, a discussion of the findings and potential threats to validity is included as well.

The paper is organized as follows. Section II presents the background for our study; standards, guidelines, and related work. The research method is described in Section III. Findings from the interviews are summarized in Section IV and discussed in Section V. Section VI provides some concluding remarks and suggests further work.

II. Background

In the following we provide an overview of important standards and guidelines for incident management in this context, as well as an overview of relevant experiences documented in literature. Based on this, we outline our expectations before the interviews.

A. Recommendations in standards and guidelines

The information security incident management process covers the complete lifecycle of an incident. ISO/IEC [3] describes this process as consisting of five phases, as illustrated in Figure 1. The Plan and prepare phase runs continuously, while the next four phases are triggered by the occurrence of an incident. Other guidelines which describe the incident management process quite similarly exist as well; although the number of phases may vary, the main ideas and activities included during the lifecycle generally resemble the ISO/IEC standard. NIST [5], ENISA [6], and SANS [7] are among the providers of the most well-known guidelines.

An organization that is about to establish its response capabilities has to perform several preparatory activities. ISO/IEC [3] provides a rather detailed description of these activities. An information security *incident management policy* should be created and integrated into other corporate policies, and this policy should reflect the organization's need for incident management and how the organization will benefit from adopting a structured approach to this. Then the information security *incident management scheme* should be described, which demonstrates the specific organization's approach to incident management - including all procedures for responding to incidents, roles and responsibilities, communication structures and reporting lines, and all other activities belonging to the complete incident management process. Establishing a specific information security *incident response team* (ISIRT) is one of the recommendations from ISO/IEC, as such a team will be specially trained for resolving incidents, and coordinating and communicating with both internal and external stakeholders. The size and structure of this team should be adjusted according to the needs of the organization. *Awareness and training* of all personnel should be performed, as all employees should be able to recognize an incident and report accordingly. Last, but not least, the ISO/IEC 27035 standard recommends *regular testing* of the incident management scheme in order to check whether the established procedures and tools function appropriately. This phase of planning and preparations is a continuous process as there is an ever-present need for updates, changes, and maintenance of policies, procedures, and practices. Incident management scheme testing and training of personnel are important in order to reveal such needs for changes, and lessons learned from actual incidents will usually also contribute in the same way.

The ISO/IEC 27035 standard addresses corporate systems in general and hence does not contain any considerations specifically related to power automation systems or industrial control systems in general. The recently published ISO/IEC TR 27019 [8] is specifically tailored for process control systems in the energy industry, but provides no additional recommendations related

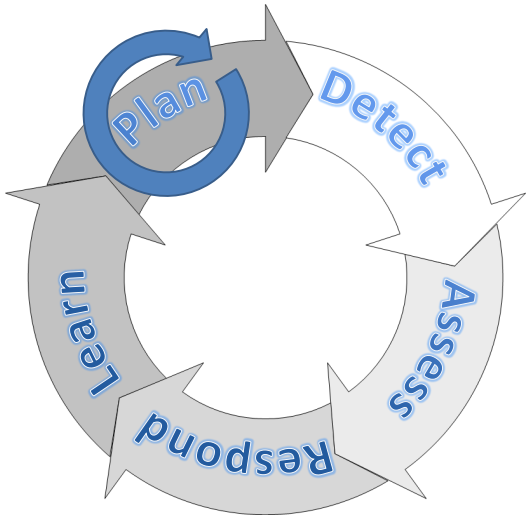

Fig. 1. The complete incident management process (ISO/IEC 27035)

to incident management beyond ISO/IEC 27002 [9]; which leaves ISO/IEC 27035 as the most comprehensive recommendations from the ISO/IEC. NIST describes a set of high-level requirements for incident response for a smart grid information system in their Guidelines for Smart Grid Security (NISTIR 7628) [10]. However, all requirements are on the governance, risk and compliance level, and are therefore more high-level than what ISO/IEC provides. They contain no specifics related to the co-operation of corporate systems and control systems. In part 3 of their Guidelines [11] NIST points out the need for research on incident response for the cross-domain of IT and power systems. More specifically, the issues of response and containment, intrusion detection and prevention, and event and impact prediction are emphasized.

B. Relevant experiences documented in literature

Experiences from literature provide more details on how planning for incident response management can be performed in practice. This literature can be used as inspiration, but also as input on which aspects of incident management are challenging and need to be given more attention. Several studies and experience reports are available, where some also provide insight to the planning phase [12]–[18]. Below we provide an overview of important findings in this literature. We organize the presentation of these findings according to the main activities recommended by ISO/IEC 27035, namely the establishment of a policy, an incident management scheme and a response team, the awareness and training activities, and the scheme testing.

The importance of establishing a team and supporting policies and documentation is emphasised also in the real world experiences documented in the literature, and detailed explanations of how this can be done are available. Metzger et al. [12] present experiences from LRZ-CSIRT[5] where a holistic approach to incident management based on ISO/IEC 27001 [19] has been implemented. They state that an efficient and effective approach for incident management is achieved through a successful combination of various reporting capabilities, automatic analysis and response, and process-oriented intervention. Recommendations from this case include the need for establishing a security incident response process and defining what a security incident is, in order to distinguish it from other types of failures and errors. Hove and Tårnes [13] point out the need for defining responsibilities, especially in organizations where IT operations are outsourced or several parties are included in operations and incident response. In complex systems it may be difficult to define such responsibilities, and it may also be difficult to know where a specific incident actually originates and thus determine who is responsible for responding [13]. Having a simple, short and common plan for incident management is recommended [17], [18]. This was considered a strength when present, and a need when not present. Without it, the approach to incident management could appear scattered and randomly structured [17].

Activities on awareness, training and incident management scheme testing seem less elaborate in existing experience literature, however the literature clearly points out the need for such activities. Flodeen, Haller, and Tjaden [14] studied an ad-hoc group of incident responders to see how a shared mental model for decision making can be developed through training. Such a shared mental model increases the performance during an incident handling process because the team manages to cooperate with limited and efficient communication. They will know where the others are in the process, the next steps, and the information required to complete the incident handling without wasting time on frequent recapture. Werlinger et al. [15] found that incident response is a highly collaborative activity, and that the diagnosis work is complicated by the practitioners' need to rely on

[5]The incident response team at Leibniz Supercomputing Centre

tacit knowledge, as well as usability issues with security tools. Hove and Tårnes [13] also found that plans and procedures are needed as a basic structure, but experienced incident handlers are much more valuable in an emergency situation. This finding aligns with theory within resilience engineering, as discussed by Pariès in Hollnagel et al. [20]. Hove and Tårnes discuss challenges of training for incident management [13]; ensuring realistic training scenarios and that the training actually provides value in real situations.

Scholl and Mangold [16] claim that a *"well-developed incident response process should be a driver for continuous improvement of enterprise security"* and that attending to small security events and early warnings can prevent major security disasters. The latter claim is in line with theory on high-reliability organizations (HROs) as described by Weick and Sutcliffe [21] and requires awareness among all employees and a reporting culture.

Most of the above identified literature considers general IT systems. The only exception is Jaatun et al. [17] who describe an incident response management process for the oil and gas industry, focusing particularly on the learning process after an incident. They found that although integrated operations in the North Sea were highly dependent on IT, there was still a great deal of mistrust between traditional process control engineers and IT personnel. Furthermore, since few cyber security incidents in this sector were systematically reported, there was a low level of awareness among upper management of, e.g., the importance of doing cyber security training drills. It seemed that some control system engineers even refused to acknowledge that their systems contained vital IT components. Jaatun et al. also found that existing reporting tools used for Health, Safety and Environment (HSE) incidents were poorly suited to reporting of cyber security incidents.

In other respects, there is a lack of studies on incident management in an operating environment with automation systems and IT systems co-functioning. Current practices, compliance to standards and/or need for changes in standards, challenges and reasons for such, and future research needs should be investigated and examined in order to provide contributions to organizations facing the reality of closely integrated IT and automation systems.

C. Expectations before the interviews

We expected to reveal weaknesses in the overall information security management system; documented policies and rules not being well-established throughout the organization, and lack of training on information security incident response. These expectations were based on our general knowledge of information security priorities in several organizations. When everything goes well, nobody offers it a thought, and it is hard to argue that more focus and investments are needed for such matters [22]. Training and improvements need to be performed on a regular basis. When everything goes wrong, it is much easier to obtain more resources, but this is rarely the time to perform training - recovery is much more important at that time to ensure business continuity. Right afterwards, someone will claim the need for training on such and similar scenarios in the future, but the everyday tasks have a tendency to receive higher priority.

We also expected to find differences between IT and control systems on several issues:

- Perceptions on what is an information security incident
- Experience in handling incidents
- Perspectives on relevance and possible consequences of different incidents

These expectations were based on the fact that there are differences between the traditions of IT and ICS, as introduced in Section I. The history of control systems, where they have been operated quite isolated from other networks, would indicate that information security incidents is an issue that they have not had to deal with before.

III. Research method

The study is based on semi-structured interviews and review of documentation [23], [24]. Six distribution system operators (DSOs) in the power industry participated in the study. They all serve more than 50.000 power consumers and are considered large in a Norwegian context.

A. Data collection

Semi-structured interviews are based on a predefined set of questions contained in an interview guide, but allow for the interviewer to add unplanned questions based on the responses provided by the interviewee [24]. Our interview guide was inspired by the ISO/IEC 27035 standard [3], and was intended to cover all phases, cf. Appendix A. However, as the interviewees are mainly managers, their responses reflected the management level perspective, and we realized during the study that we did not receive as much detailed information on the response activities as we first expected.

The interviews were carried out June-December 2012 at the various DSOs' premises respectively. All interviews were voice recorded and transcribed. The study was registered at the Data Protection Official for Research[6] and all interviewees signed a consent agreement according to the privacy regulations. One test interview was carried out in DSO B, without the use of voice recording. This interview is not included in the data material, but used as a test of the interview guide and training for the

[6]http://www.nsd.uib.no/personvern/en/index.html

TABLE I
THE DISTRIBUTION SYSTEM OPERATORS (DSOS) INCLUDED IN OUR STUDY

DSO	Role of interviewees	Documentation received	IT operations outsourced	Required NDA
A	IT, IT sec, IT operations, control systems	Information security instructions, Plans for preparedness in IT systems	yes	no
B	IT, IT sec, control systems	no	no	no
C	Corporate IT, IT in branch company, control systems	no	yes	no
D	IT, IT sec, control systems	no	yes	yes
E	IT, IT sec, control systems	Information security instructions, Plans for preparedness in control systems	no	yes
F	IT sec, control systems, quality & risk	Information security policy, Information security events (quarterly report Q2-2012)	yes	yes

interviewer. The test interviewee was not interviewed again, but he is included in the mailing list of interviewees who receive information and updates from the study.

Data triangulation is a way of enhancing the rigour of the research [24], which means using multiple methods for data collection. In addition to the interviews, we thus asked the DSOs for the following types of documents:

- Information security policy
- Information security instructions
- Plans for continuity and preparedness
- Plans for information security incident management
- Periodical reports on information security incidents
- Other related documents they may have

Three of the DSOs provided us with some documentation (c.f. Table I). Confidentiality issues prevented the other three DSOs from sharing documentation. Non-disclosure agreements and encrypted electronic transfer were not sufficient instruments for overcoming the confidentiality issues[7].

B. Data analysis

The analysis followed an integrated approach, which combines the inductive development of codes with a start list of categories in which the codes can be inductively developed [26], [27]. It was mainly performed by one researcher due to confidentiality restrictions posed by three of the participating DSOs (D, E, F, c.f. Table I)[8]. Two fellow researchers were involved in discussing coding categories and findings, and writing up this report. They had access to the transcriptions from the interviews conducted in the other three DSOs (A, B, C, c.f. Table I). The software tool NVivo[9] was used for the data analysis.

C. Industrial case context

Six DSOs are included in the study, and they were selected for being among the largest DSOs in the country, as well as being partners in the national research project DeVID. Three different roles from each DSO were interviewed; IT manager, IT security manager, and manager of control systems. One exception is DSO F, where the IT manager was unable to participate, and we talked to the manager for quality and risk instead. In one of the DSOs we also interviewed one member of the technical IT staff in addition to the IT manager. In total, 19 interviews were carried out. As we address incident management from the information security management perspective, only managers were included in the interview study. If we were to investigate in further detail the technical response activities performed when an incident occur, we would have had to include technical IT staff and preferably also representatives from external IT suppliers in the cases where the DSOs have outsourced large parts of their IT operations. In order to get the whole picture of IT and power automation, we included managers from both areas.

More DSOs than these six are partners in the national research project DeVID and could hence easily have been included. However, after the completion of the planned interviews in the six DSOs, saturation was reached [28]. For the perspectives

[7]It must however be noted that just the day after my request for documentation, the authorities sent an e-mail to all units that are part of the national emergency preparedness organization for power supply, which all the DSOs in this study are part of, encouraging them to be critical to all requests for sensitive information. The authorities state that information sharing is not prohibited, but should be carefully considered in each case. As information security researchers we should appreciate such caution regarding sharing of confidential documents, although it poses limitations to the data triangulation. Kotulic et al. [25] point out this challenge of obtaining sensitive data as limiting to research on information security management in general and recommend focusing on a few selected companies. This opens for building trust between the company and the researcher, which will ease collection of sensitive data. Also, the companies in focus can be more involved in discussing and approving the results.

[8]All DSOs are partners in the DeVID project. Some considered the confidentiality agreement for the project consortium to be sufficient for this interview study, while others required the signing of an additional non-disclosure agreement (NDA) for the interviewing researcher.

[9]http://www.qsrinternational.com/

TABLE II
DISTRIBUTION OF INTERVIEWEES PER ORGANIZATION

DSO	IT manager			IT Security Manager			% IT security
	Parent co	Branch	Outsourced	Parent co	Branch	Outsourced	of full position
A			x[a]		x[a]		5%
B	x[b]			x[b]			100%
C	x[b]	x[a]					
D	x[a]				x[b]		10-20 %
E	x[a]				x		100%
F						x [a]	50%

[a] Only administrative system
[b] Both IT and ICS

of IT managers and IT security managers, saturation was actually reached before all the planned interviews were completed, as their responses were fairly aligned. The need for information from control room managers still called for completing the interviews in all six DSOs.

All the DSOs are organized as a corporation where the power supply infrastructure is taken care of by one branch company. Other branch companies may be within power production and broadband. Four out of six have outsourced their administrative IT services to an external supplier, but all these external suppliers are 100% owned by the DSOs respectively, due to their past as an internal IT department. The other two operates the administrative IT systems themselves. Control systems are operated internally by all the DSOs.

All the control system managers belong to the branch company[10]. They are responsible for the daily operations of the control systems, including information security issues. Even in the cases where IT managers or IT security managers are said to be responsible for this, it is the managers of control systems who in practice execute this authority. A brief overview of the participating organizations is presented in Table I, and roles and placement of interviewees within each organization is explained in Table II.

IV. FINDINGS

A. Dependency on IT

The responses indicate that the DSOs can better endure unforeseen downtime in their power automation systems than in the administrative IT systems. All the IT managers and IT security managers claim that their organization is 100%, or close to 100%, dependent on IT systems. The business may run for some days without IT systems, but several challenges will occur quite soon. Planning, follow-up, and maintenance will be impossible. If maps of the distribution grid are not available, no digging can be done in a certain area, which again may stop construction work. If invoicing is impossible, the cash flow will stop; this is when the IT breakdown really manifests itself.

The control system managers also state a 100% dependency of IT, although they add that unavailable IT systems do not automatically cause power failure for customers. The distribution grid can be operated manually even if the control room or other parts of the SCADA systems are unavailable, as this is a requirement in the national regulations. However, the customers will be the most important failure detection mechanism and the DSOs will face the challenge of making the right prioritizations based on information from the customers, as opposed to having functioning monitoring systems that automatically detect failures and provide richer background information on the failures. The length of the period that the DSOs are able to operate manually depends on available personnel for fixing failures, but two-three days would be manageable. If the amount of failures is too high, they are not able to keep up, which might result in a considerably reduced quality of service for customers. With a smaller amount of failures, manual operation may be possible for a long time.

The term *IT systems* is interpreted differently among the interviewees dependent on their work position. IT managers do not necessarily include SCADA systems in their definition. For control room managers, IT systems equal SCADA systems.

B. Definition of an incident

The responses indicate that IT managers and IT security managers have a much more uniform comprehension of the concept of information security incidents than control room managers. There are large variations among control system managers when they are asked to define an IT security incident. None of them provide a clear definition, and they all state that this term is not defined in the organization. One (A) thinks of it as malicious attacks, while he considers unavailability due to digging or technical failures to be outside the scope of information security. Four respondents think of it as unwanted occurrences in the IT systems, including breaches of policy or procedures, computer viruses and intrusions, and the last one (E) explains it more specifically as an occurrence that can affect functionality and/or compromise sensitive information.

[10]The one from E belongs to a the branch company for power production where the IT operations are located, same as for the IT security manager from E.

Only the IT manager in C used the terms confidentiality, integrity and availability when defining an IT security incident. The others have similar perceptions, without providing a clear definition. Examples of incidents are mentioned, like disclosure of confidential information to unauthorized persons, breach of procedure, intrusions, sabotage, computer viruses, both malicious and accidental occurrences.

"Good question. I have never thought of that."

— IT manager (A) when asked to define an IT security incident

Among IT security managers only the one from F uses the terms *confidentiality, integrity and availability*. All the others claim that their organization does not have a clear definition of what comprises an incident, but like the IT managers, the IT security managers also provide several examples of IT security incidents, like hardware thefts, hacking, viruses and sabotage. This aligns with the documentation studied. The information security policy from F states a clear definition as provided by the IT security manager, and also *authentication* is included in the written policy. The information security instructions from A and E do not contain any definition. However, several examples of information security incidents are listed in the documentation we received, as reflected by several of the informants.

A common impression among control room managers is that IT incidents have never occurred in their systems. IT security managers, to the contrary, claim that several incidents occur every week. Control room managers claim they have never experienced disruptions in power supply due to information security incidents. The power automation systems are extremely robust and resilient towards incidents involving individual components. Physical damage due to stormy weather may occur, but they do not refer to this as an information security issue.

C. Worst case scenario

Almost all interviewees state that the worst incident they can imagine is if someone hacks the power automation system, gains control of power switches and can control the power distribution system. Attackers could cause outages in large cities in a few minutes if they have the right access. They could also do the opposite; switch the power on in a part of the grid that is without voltage due to maintenance and hence cause physical harm or death to maintenance workers. This is especially mentioned by the control system manager in D. Even though several security mechanisms are in place to prevent such and similar scenarios, it is stated by the interviewees that they might still occur, even though the probability is quite low. Also, as the control system manager in F states, the attack force obtained through a combination of foreign governments and criminal actors exceeds the response capabilities of most organizations.

Other worst case scenarios mentioned include compromised customer databases with large amounts of personal information; complete deletion of databases (and all related backups) containing all information on the physical power grid; minor errors in the billing system for a long time such that rollback is impossible when the errors are finally detected; compromised information on power distribution that could be used to attack certain customers; misuse of the disconnection function in smart meters that could result in outages without the SCADA system being involved; and fire or natural disasters that destroy buildings where the control room is located.

The IT security manager from E points out that sensitive information is not handled satisfactorily. He believes that cloud services are widely used, without this being approved as acceptable and secure storage. Employees require availability of information and flexibility in when and where to work, and take with them information without considering possible implications on information security. Such breaches may have large financial consequences to the organization if for example tender documents have been compromised.

The IT security manager in F states that the combination of incidents is the worst thing, for example a hacking attack and really bad weather causing logical errors and physical damage at the same time.

D. Documentation of plans and procedures

Three of the four DSOs that have outsourced their administrative IT systems (A, C, D), lack plans for responding to incidents and seem to rather expect the IT supplier to have such plans in place[11]. The information security instructions from A contains only reporting procedures for users. However, some DSOs (A, B, D) are currently working on documenting their plans and procedures for the first time, both for IT and control systems. They have been trusting their employees to know what to do, but have realized that they also need a certain documentation base in place. It is however not clearly stated who will actually develop unified plans that take both IT and control systems into account. The ISO/IEC 27001 standard is mentioned as being used for identifying issues to be documented. The other DSOs do have reporting procedures and/or continuity plans in place.

One IT security manager (F) states that his organization has an information security policy and procedures for incident management in place. This was also among the documentation we received. However, the control room manager from the same organization is not familiar with the existence of this documentation. The control room manager in B is aware of the

[11]Whether this also goes for the fourth DSO in the same outsourcing situation is unclear, as the IT manager was not among the interviewees, and the IT security manager belongs to the external IT supplier.

existence of such plans in his organization, but they originate from the IT department and do not consider automation systems specifically. He would like to have similar documentation for his systems as well. He does not seem to be aware of the procedures currently being prepared as reported by the IT security manager.

In E they have clearly defined procedures for the administrative systems and security instructions for the power automation systems. Their control room manager states that documentation needs to be combined with highly competent personnel, because it is impossible to write detailed procedures for any possible incident.

Several interviewees admit that plans are not commonly used, either because they are non-existent or because incidents occur quite rarely. The one from IT operations in A however says that they practice quite frequently and mentions that employees are invited to hand in their laptop during summer holiday for a clean-up. Then the technical personnel familiarize themselves with the computers, analyze them and are able to test different tools. The purpose is not to reveal any breaches by the employees but to practice and experience technical support and maintenance issues.

The ISO/IEC 27035 standard is not mentioned by any of our informants. We did not ask specifically whether they were familiar with it, but it was never brought up during any of the interviews. This may indicate that the standard is not used by the organizations. It might be the case that the informants did not find an opportunity to mention it among all the questions that were asked, although this does not appear as the most plausible explanation, as the use of such a standard is closely linked to the existence of plans and procedures, which was a topic in all interviews.

> *"This I have never asked for, to see the procedures for responding to an information security incident. Maybe I should."*
>
> *— IT security manager (D)*

E. Preparedness for worst case scenarios

Three IT managers (B, D, E) claim that they will be able to respond satisfactory to a worst case scenario, due to their well organized and planned emergency preparedness in general, although they have some weaknesses related to IT-specific preparedness. They are currently working towards a more systematic IT security preparedness as well, and one (B) is planning a physical backup site, having identified this as a need in order to be better prepared. The IT security manager from B supports his IT manager in this view of them being prepared to respond to a worst case scenario. The IT security manager from D is more reluctant to claim that they are well prepared; he says that they lack practice and well established procedures. However, he feels confident that they will be able to improvise. He is not worried about the control systems in case of an incident, as this can be disconnected and operate offline. The IT security manager in E agrees with his IT manager in that they are prepared, although it should be noted that they present quite different scenarios to be the worst cases to occur (compromised sensitive information vs. sabotage/natural catastrophe/hacking attack).

The other IT managers assume that their organization will not be able to respond appropriately to a worst case scenario. As reasons they state that there are too few preparedness training drills, and that those that are performed have a too limited scope. Some perform dry runs from time to time.

The control system manager from D believes that their current procedures and practices would suffice if the worst case scenario should occur. However, as he states, it will be a future task to consider whether the response was appropriate or poor.

Several of the interviewees state that the control systems can be disconnected from the outside world and continue operation, something they perceive as an efficient response to incidents where the control systems are hacked. One (A) however points ut that this does not solve anything; it would stop the attack, but it would prevent you from further investigating the incident with respect to who is behind it and what could be the consequences.

F. Training

None of the IT managers or IT security managers report that they perform regular training exercises where an information security incident creates the basis for the scenario. But the authorities initiate general emergency preparedness exercises from time to time, and in some cases the scenario is based on such an incident.

The IT security manager in A expects their external IT supplier to perform training. However, the IT manager in A, who is the manager of this external IT supplier, claims that they never perform such training. The IT manager from C (branch company) states the same; that training for incident management is never performed. The corporate IT manager in C supports this fact that training is not performed, but he adds that they have had their share of incidents. He would like to see more training drills instead of the real incidents. Some IT security managers (D, E) agrees that training should be performed more often. "Fumbling and hubbub" constitute the most useful exercises, as put by the IT security manager from E.

> *"We are not good at post-evaluating real incidents and consider them as training exercises, we are too solution-oriented."*
>
> *— Corporate IT manager (C)*

Different reasons are given for the lack of training: training activities have not been prioritized, other tasks receive higher priority, and training involves a certain cost.

"There are too many other tasks, so we haven't had the time for it. Maybe that's wrong, not to prioritize it."

— Control system manager (C) on training exercises

The IT security manager in F argues that training is assigned a low priority due to the fact that real incidents rarely occur, hence they do not feel the need for being better prepared for responding efficiently. Still, their information security policy states that the plan for emergency preparedness is to be tested regularly, and that IT/infrastructure should be included.

In B they run comprehensive preparedness exercises internally in addition to the ones initiated from the authorities, as reported by their IT manager and IT security manager. These are not specifically related to IT security incidents, but there have been scenarios that include such elements, like fire in a building where the data centre and/or communication systems are located. Both dry runs and more realistic drills are performed.

Among the control room managers, the experiences with training vary. In E they manage to look at real incidents as training, adding some effort to the response activities; hence feeling more confident afterwards that their systems function as intended. The control room manager in F reports that they perform regular exercises on responding to communication breaches in the control systems. This aligns with the requirements in their plan for emergency preparedness as well. They have never considered training for information security incidents, but during the interview he realizes that the consequences, and hence the response activities, could be similar for those two scenarios. Hence, their regular training does strengthen their information security incident response capabilities as well as their general emergency preparedness. On the other hand, the other control room managers (A, B, C, D) state that they do not perform training for information security incident management. Reasons provided include merging of companies, moving, cost, time, and workload. Also the number of incidents experienced is quite low, so the need for training has not been identified in all DSOs. All these four interviewees feel that their training efforts are not satisfactory, but only one (C) states that they intend to improve in this area. *The personnel operating the control systems would benefit from training on scenarios like "what do we do if the control systems break down?",* reports the control manager from C.

V. Discussion

This paper set out to identify how planning and preparatory activities for information security incident management were performed in organizations that depend on successful cooperation between people working on conventional IT systems and ICS (Research Question 1). It also set out to identify differences in the planning and preparatory activities performed in these two disciplines (Research Question 2). The results show that current planning and preparatory activities are limited, at least compared to the recommendations in current standards and guidelines. ISO/IEC 27035 recommend activities related to the following: establishment of a policy, an incident management scheme and a response team, awareness and training, and scheme testing. In the following we summarize current practice on activity areas recommended in ISO/IEC 27035, before outlining the differences identified between the practices of IT and ICS staff. Then we move on to discussing the validity of our findings.

A. Current practice

We expected to find that documented policies were not widely established throughout the organizations, as well as a lack of training on information security incident response. These expectations were confirmed in the interviews.

In general, responsibilities in information security incident management seem to be inadequately established. This seems especially to be the case when IT system maintenance is outsourced. Documented plans and procedures for incident management in the IT systems do not widely exist. Where such plans do exist, some informants state that they do not sufficiently consider ICS. Just as often as answering yes/no to the question on whether plans exist, the interviewees started describing their plans. This suggests that the personnel most frequently involved in incident management have tacit knowledge and experience in the necessary actions to be taken in case an incident occurs. In daily practice this can be sufficient, as long as this personnel is available when incidents occur. Some DSOs have however found that they cannot solely rely on tacit knowledge for this, and are in the process of creating plans. Still they are aware that you cannot document everything, and have to rely on competence of personnel in addition to documentation.

Although the DSOs are highly dependent on the availability of competent personnel should an incident strike, they only report on limited awareness and training activities on information security incident management. In cases where procedures are documented, these do not seem to be well established or, in some cases, even known by staff expected to work according to the procedures. Any training activities performed seldom take information security incidents into account. Some of the activities reported as training in the interviews are also not really tailored to incident management, but are rather part of general computer maintenance. The reported reasons for not performing more training on information security incident management include cost and time issues, but in general it does not seem that they see the need for more focus in this area. Currently they experience a limited number of incidents.

Clearly, training activities seem to be difficult to prioritize. Whether training is also difficult to carry out is not clear. The interviewees who report that they perform drills from time to time do not report on specific challenges related to planning

them or going through with them. However, training might be continuously postponed due to the lack of knowledge on how to plan and/or accomplish such trainings.

Incident management scheme testing seem not to be performed by the DSOs. This can also be related to the unavailability of a scheme to test. But despite a general lack of plans for handling information security incidents, and a lack of training on this, quite a few DSOs still seem to have a relatively high degree of confidence that they can handle even a worst case scenario. They trust the competence of their employees and their ability to improvise and find solutions if an incident should occur. They also rely on their ability to disconnect their most critical systems from the outside world in case of a serious incident.

The findings in this survey seem to be in line with documented experiences in literature (see Section II-B), although the DSOs seem to lag behind on the establishment of policies, an incident management scheme and a response team [12], [13], [18]. Hove and Tårnes [13] documented specific challenges relating to outsourcing, and also the importance of having experienced incident handlers over a strict reliance on documentation. Lack of training for incident response is also identified in previous studies and experience reports. The challenges identified by Hove and Tårnes [13] when it comes to training (realistic scenarios, value for real situations) did however not come up in the performed interviews.

The relatively high trust in own abilities to handle worst case incidents can probably be explained by unrealistic optimism in risk perception in the information security domain, as documented in the study by Rhee et al. [29]. In order to mitigate this optimistic bias, they suggest that organizations perform more security awareness training and apply a more systematic approach to information security management. Such an approach seem to be currently lacking in the DSOs taking part in this study. The awareness by some of the interviewees on the importance of competence and ability to improvise is in line with resilience theory [20], but there seem to be a lack of understanding of what actions need to be in place in order to improve resilience in an organization, including risk awareness, response capacity and support [30].

B. Differences between IT and ICS

Table III presents a brief overview of the findings from our study of DSOs. A previous study in the oil and gas industry [17], where the implementation of integrated operations was in progress at the time, revealed similar gaps between IT and ICS as our recent study in the power industry. This gives us reasons to believe that similar organizations in other industries as well would report along these lines, given that the integration of IT and ICS has reached the same stadium as in the power industry.

We expected to find differences between IT and ICS staff when it came to perceptions of what an information security incident is, experience in handling incidents, and in the percieved consequences of incidents. As Table III shows, we were correct in our expectations when it comes to definitions and percieved consequences of incidents. From an IT perspective, such incidents happen frequently, and are concerned with compromise of information. From an ICS perspective the understanding of what an information security incident is seem to be more unclear, and they are mainly concerned with consequences for power supply. Variations existed among control room managers, and they commonly claim that information security incidents have never occurred in the control systems. IT managers and IT security managers are much more aligned, which could be explained by their common background and experience with the same type of IT systems and the same kind of information security threats. Control room managers give mixed responses on the relevance of minor information security incidents, but they all suggest malicious hacker attacks where the hacker gains control of power switches as the worst case scenario. This indicates that they have a fairly good understanding of the vulnerabilities and existing threats to their control systems in the situation of dependency of conventional IT systems. As such, they are aligned with the IT managers and IT security managers.

Also regarding experience in handling incidents, the findings resemble our expectations. Information security incidents occur frequently in the administrative IT systems in the DSOs, while rarely, if ever, in the control room. However, they do experience incidents in the control room as well, like component failures and communication breach, but these incidents are not defined as being information security incidents. Still, the consequences posed by all these examples might be quite similar. This suggests that control room managers and their operators might be better prepared for responding to information security incidents than the first impression might indicate. However, as the definition of an information security incident is not all clear, the biggest challenge of incident response in the control room might be to actually recognize such an incident and be able to determine the most appropriate first steps for the response phase.

Procedures for general emergency preparedness are usually well established and well practiced among control room operators, as reported by control room managers. The DSOs are required to perform exercises regularly, as a measure for ensuring continuous power supply. Traditional exercises have however rarely been based on incidents caused by IT systems. IT and ICS are viewed as two separate parts of the organization, and there has been limited collaboration between the two.

C. Threats to validity

Construct validity concerns whether a study measures what it sets out to measure [24]. Interviewees may be biased, either consciously or unconsciously [31]. The topic being information security incidents could increase this bias as well; their conscious or unconscious desire to make their organization and themselves look good from the outside. Our impression is that they were being honest in their reportings as several of the interviewees did not report a perfect situation, rather lackings in a

TABLE III
SUMMARY OF FINDINGS

	IT systems	**Control systems**
Dependency on IT	Claim to be 100% dependent, can endure for some days, until cashflow stops.	Claim to be 100% dependent, but can operate power grid manually without control room. Endurance of manual operation is determined by number and severity of failures that occur.
Definition of incident	Confidentiality, integrity, availability mentioned by some. Both malicious and accidental occurrences - unwanted. Occurs frequently.	No common definition exist in the organizations. Malicious attacks, unwanted occurrences in the system. Occurs rarely, if ever.
Worst case scenario	Compromised/deleted databases with customer information and/or information on the physical power grid	Malicious hacker attacks in control systems, gaining control of power switches, causing outages.
Documented plans	Not widely established. In progress in some DSOs.	Established in one DSO, otherwise in progress or non-existing.
Preparedness for worst case	Various perceptions: Well-organized and planned general emergency preparedness, and/or ability to improvise. Also reported doubt on own preparedness due to lack of training.	Current practice and competence is perceived as sufficient. Disconnecting the control room is highlighted as the most appropriate and plausible measure towards worst case scenario (malicious hacker attack).
Training	No regular drills based on information security scenario. Regular general emergency preparedness exercises; occasionally, these deal with information security/IT incident.	Regular general emergency preparedness exercises; information security never forms the basis.

number of areas. Some even expressed their gratitude for us performing this study, as it gave them an opportunity to discuss these issues internally. Being able to point to us as external, independent researchers, strengthened their message.

All interviewees belong to a management level in the organization. The IT security manager often reports to the IT manager, but there are still employees on lower levels performing a large part of the daily tasks within incident management. Not including such employees as interviewees is an obvious limitation of this study, as the managers might provide information on how things should be done, not just on how things actually are being done. However, it was necessary to make such a limitation due to time constraints. Also, the planning and preparations activites, as this paper reports, are the responsibility of the managers. So for this part of the study, the selection of interviewees appears appropriate.

An alternative strategy would be to study only one or two organizations in depth, and then include more employees from each organization as interviewees. This would probably make us better able to say something about differences between written plans and procedures and actual daily practice. However, we wanted to cover a larger number of organizations in order to see what is widespread current practice.

Data triangulation [23] increases the quality of data as it allows a phenomenon to be studied from different perspectives. Interviews and documentation provides two different views on incident management, as the interviewees would describe their practice as they know it, while documentation will show the planned procedures. We did not distribute the interview guide in advance, as we did not look for the ”correct” answers, but rather the interviewees’ perceptions, understandings and actual practice. Then we studied the received documentation to see whether there were any significant differences between the two. A third source of evidence was considered, but has unfortunately not been feasible: participating in a post-incident evaluation meeting at a specific DSO. This would have provided us with detailed information on how an actual incident was responded to. The DSOs have expressed willingness in including us in such a meeting, but we have not been able to follow-up on this as it would require us to be actively asking for it regularly; we would not expect them to call us.

We did not interview the IT manager in DSO F as he was not able to make it, even though we did schedule the interview in advance. We instead got to talk to the Manager for quality and risk. We asked each DSO for specific roles and described the purpose for this, but we could not control in detail who were identified by each DSO to participate. As most of the interviews required travelling and hence planning ahead, we were not able to go back to the DSOs in order to meet the most appropriate person if he was not present on the agreed time and date. We asked the IT manager in DSO F to respond to our questions in writing, because that would give us a richer data material than no response at all. However, we never received anything from him.

All interviewees were provided with a draft of this paper, and hence given the opportunity to comment on the results. This is referred to as member checking [24], and is a strategy for reducing researcher bias. In our study where one researcher did most of the analysis, this was especially important. It also shows that we value the contributions of our informants. We received feedback regarding the case context description, which we updated accordingly.

External validity refers to the degree to which the findings from a study can be generalized to other settings [24]. Our study is restricted to large DSOs and the roles of the requested interviewees were clearly defined. We have provided a detailed description of the industrial case context (cf. Section III, which is of great importance when considering whether our results

are transferrable to a given setting. As our expectations regarding findings were generally met, it may be assumed that the participating DSOs do not stand out in any particular way compared to similar organizations. There is a lack of similar studies[12] on incident management in organizations depending on successful collaborations between IT and ICS, hence we believe that our study should be repeated for similar and slightly different case contexts than ours. Generalizability will be strengthened by increasing the number of studies.

VI. Concluding remarks and further work

This paper has presented findings related to the planning and preparations activities for information security incident management. There are differences between the IT and ICS disciplines in practice, as we expected beforehand. As the Smart Grids emerge, IT will be permeating the control systems even more than today; more commercial off-the-shelf products, more connectivity, and more integration [1]. Further studies are required to investigate how these differences should be addressed for a unified approach to incident management to be achieved.

> *"The greatest challenge is that they don't understand how IT intensive their new world will be."*
>
> *— IT manager on control room operators and the future with Smart Grids*

Training for IT security incidents is reported as challenging; especially being able to prioritize it among several pressing tasks. However, general emergency preparedness exercises are frequently performed. Future work should investigate why training for IT security preparedness is more difficult and how knowledge could be transferred from the areas of general emergency preparedness exercises, industrial safety training and resilience, in order to design and implement training programs for organizations where IT and SCADA systems and staff need to collaborate.

> *"The big profit for the industry will be in accomplishing successful interaction between IT and power. That will also gain information security in smart grids."*
>
> *— IT manager*

The ISO 27035 was not brought up in any of the interviews. This calls for an investigation on the knowledge of this standard and to which extent it could assist DSOs and similar organizations in improving their information security incident management process.

Activities performed during and after an incident were also covered in the same interviews, and these findings will be presented and discussed in a follow-up paper. We have recently performed additional interviews in small DSOs, where *small* is defined as *supplying less than 10.000 power consumers*. The follow-up paper will also summarize findings from these interviews, including a comparison of large and small DSOs on their approaches to incident management.

Acknowledgment

We are grateful to the distribution system operators who contributed with informants for our interviews.

References

[1] M. B. Line, I. A. Tøndel, and M. G. Jaatun, "Cyber security challenges in smart grids," in *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, Dec. 2011.
[2] Éireann P. Leverett, "Quantitatively Assessing and Visualising Industrial System Attack Surfaces," University of Cambridge, 2011.
[3] "ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management," 2011.
[4] M. B. Line, "A Case Study: Preparing for the Smart Grids - Identifying Current Practice for Information Security Incident Management in the Power Industry," in *Seventh International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2013.
[5] T. Grance, K. Kent, and B. Kim, "NIST SP 800-61: Computer Security Incident Handling Guide," National Institute of Standards and Technology, 2008.
[6] ENISA, "Good practice guide for incident management," 2010.
[7] P. Kral, "The Incident Handler's Handbook," SANS Institute, Tech. Rep., 2011.
[8] "ISO/IEC TR 27019:2013 Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry," 2013.
[9] "ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management," 2005.
[10] NIST, "7628-1: Guidelines for Smart Grid Cyber Security," National Institute of Standards and Technology, 2010.
[11] NIST, "7628-3: Guidelines for Smart Grid Cyber Security," National Institute of Standards and Technology, 2010.
[12] S. Metzger, W. Hommel, and H. Reiser, "Integrated Security Incident Management – Concepts and Real-World Experiences," in *Sixth International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2011, pp. 107–121.
[13] C. Hove and M. Tårnes, "Information Security Incident Management: An Empirical Study of Current Practice," Norwegian University of Science and Technology, 2013.
[14] R. Floodeen, J. Haller, and B. Tjaden, "Identifying a Shared Mental Model Among Incident Responders," in *7th International Conference on IT Security Incident Management and IT Forensics*. IEEE Computer Society, 2013.
[15] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov, "Preparation, detection, and analysis: the diagnostic work of IT security incident response," *Information Management & Computer Security*, 2010.
[16] F. Scholl and M. Mangold, "Proactive Incident Response," *The Information Systems Security Association Journal*, 2011.
[17] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tøndel, and O. H. Longva, "A framework for incident response management in the petroleum industry," *International Journal of Critical Infrastructure Protection*, vol. 2, pp. 26–37, 2009.

[12] With the exception of the related work of Jaatun et al. [17]

[18] J. Cusick and G. Ma, "Creating an ITIL inspired Incident Management approach: Roots, response, and results," in *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP*, 2010, pp. 142–148.
[19] "ISO/IEC 27001:2005 Information security management systems - Requirements," 2005.
[20] E. Hollnagel, J. Pariès, D. D. Woods, and J. Wreathall, Eds., *Resilience Engineering in Practice - a Guidebook*. Ashgate Publishing Ltd., 2011.
[21] K. E. Weick and K. M. Sutcliffe, *Managing the unexpected*. John Wiley, 2007.
[22] N. P. Repenning and J. D. Sterman, "Nobody ever gets credit for fixing problems that never happened: creating and sustaining process improvement," *IEEE Engineering Management Review*, vol. 30, pp. 64–64, 2002.
[23] R. K. Yin, *Case Study Research - Design and Methods, 4th ed.*, ser. Applied Social Research Methods. SAGE Publications, 2009, vol. 5.
[24] C. Robson, *Real world research*, 3rd ed. John Wiley & Sons Ltd., 2011.
[25] A. G. Kotulic and J. G. Clark, "Why there arent more information security research studies," *Information & Management*, vol. 41, no. 5, pp. 597 – 607, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378720603000995
[26] R. Bogdan and S. Biklen, *Qualitative research for education: an introduction to theory and methods*. Allyn and Bacon, 1982. [Online]. Available: http://books.google.no/books?id=wIOcAAAAMAAJ
[27] J. Lofland, *Analysing social settings*. Wadsworth Pub, 1971. [Online]. Available: http://books.google.no/books?id=fIOjKQAACAAJ
[28] G. Guest, A. Bunce, and L. Johnson, "How many interviews are enough? An experiment with data saturation and variability," *Field Methods*, vol. 18, no. 1, February 2006.
[29] H.-S. Rhee, Y. U. Ryu, and C.-T. Kim, "Unrealistic optimism on information security management," *Computers & Security*, vol. 31, no. 2, pp. 221 – 232, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404811001441
[30] K. Bernsmed and I. A. Tøndel, "Forewarned is Forearmed: Indicators for Evaluating Information Security Incident Management," in *Seventh International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2013.
[31] T. Diefenbach, "Are case studies more than sophisticated storytelling?: Methodological problems of qualitative empirical research mainly based on semi-structured interviews," *Quality & Quantity*, vol. 43, no. 6, pp. 875–894, 2009. [Online]. Available: http://dx.doi.org/10.1007/s11135-008-9164-0

APPENDIX A
INTERVIEW GUIDE

Individual

1) How many employees are there in your organization?
2) Which position and/or role do you have?
3) For how long have you had this position?
4) Which systems and procedures are within your responsibility?
5) Can you describe how your position connects to the work related to security, ICT and automation systems?

ICT security incidents

6) To which degree does the organization depend on ICT?
7) How would you define an ICT security incident?
8) Can you describe your latest ICT security incident?
   - How was this incident responded to?
   - How well did the response work?
   - Why did the response work as it did?
9) What is the worst ICT security incident your organization could experience?
10) If you think about how the latest ICT security incident was responded to, would this be sufficient to handle the worst possible ICT security incident?
    - Would you have done the same if it was a targeted hacker attack?
11) How frequently do you experience ICT security incidents?
    - If you have never experienced ICT security incidents, what could be the reasons for that?
12) What kind of ICT security incidents do you experience?
    - What kind of consequences are typical for this kind of incidents?

Responding to ICT security incidents

13) Which plans exist for ICT security incident management?
14) Are the plans used in practice?
    - If not, why not?
15) Do you perform training on incident management?
    - If yes, how? (Scenarios, exercises, courses?)
    - If not, why not?
16) How are ICT security incidents usually detected? (Automatic tools? Intrusion detection systems? Firewalls? Users? Manual audit of logs?)
17) How are ICT security incidents initially reported?
18) Who is involved in responding to ICT security incidents?
19) Do you experience challenges related to cooperation on responding to incidents?
    - If yes, what kind of experiences? (Are they related to communication? Terminology? Responsibilities? Knowledge and experience? Procedures?
20) What kind of supplementary work is performed when regular operation is restored?
21) How are ICT security incidents registered and reported afterwards?
22) Is information on incidents reported to top management?
23) Is information on incidents disseminated to end-users, internally or externally?
24) Do you report ICT security incidents to the police?
25) Are the experiences from ICT security incidents used as input to further risk assessments and improvements of procedures afterwards? (Or is incident response mainly ”‘firefighting”’?
    - If yes, which parts of the organization are involved in this process?
26) Do you have any numbers for the costs of ICT security incidents?
    - If yes: How frequently and how are these followed-up? Who is responsible?

27) Did you establish any other indicators or measurements for ICT security incidents? (E.g., downtime due to incidents, number of incidents per month)
    - If yes: How frequently and how are these followed up? Who is responsible?

Possible improvements

28) What are the most important actions performed in order to restore regular operation and limit the consequences from an ICT security incident?
29) Do you see any possible improvements to how you respond to ICT security incidents?
    - If yes, which?
30) The Smart Grid leads to a closer integration of ICT and automation systems in the future. How do you think this will affect ICT security incident management?
31) Is there any cross-organizational cooperation in the industry regarding information security? (Work groups, seminars, regular meetings?)
    - If yes, to which degree is ICT security incident management on the agenda?